

**IN THE UNITED STATES DISTRICT COURT FOR THE
SOUTHERN DISTRICT OF NEW YORK**

UNITED STATES OF AMERICA,

Plaintiff,

v.

ANTON PERAIRE-BUENO, and JAMES
PERAIRE-BUENO,

Defendants.

Case No.: 1:24-cr-00293-JGLC

[FILED PARTIALLY UNDER SEAL]

DEFENDANTS' OPPOSITION TO NON-PARTY 1'S MOTION TO QUASH

TABLE OF CONTENTS

BACKGROUND	2
ARGUMENT	4
I. THE PROTECTIVE ORDER SUFFICIENTLY ADDRESSES CONCERNS ABOUT CONFIDENTIAL BUSINESS INFORMATION.	5
II. THE COURT SHOULD DENY THE MOTION TO QUASH AS TO THE REQUESTS FOR SOURCE CODE (REQUESTS 1-3).....	7
A. The Source Code for the MEV-Bot and the Smart Contracts Is Relevant.....	7
B. The Publicly Available Bytecode and Literature on the MEV-Boost System Do Not Provide the Requested Information.	10
C. Requests 1-3 Are Not Overbroad.....	11
D. Non-Party 1 Does Not Face Undue Burden.....	12
E. If the Court Quashes Requests 1-3, the Government Should Be Precluded from Presenting Evidence or Argument on These Issues.	13
III. THE COURT SHOULD DENY THE MOTION TO QUASH AS TO THE REQUESTS FOR COMMUNICATIONS (REQUESTS 4-7).	13
A. The Communications Are Relevant.....	13
B. Non-Party 1 Provides No Basis for the Redactions at Issue in Request 4.....	16
C. The Specificity Requirement Is Satisfied, and the Requests Are Tailored in Time and Subject Matter.....	17
D. The Communications Are Potentially Admissible.	18
IV. THE COURT SHOULD DENY THE MOTION TO QUASH AS TO REQUESTS 8 AND 9.....	19
CONCLUSION.....	21

TABLE OF AUTHORITIES**Page(s)****CASES**

<i>Old Chief v. United States</i> , 519 U.S. 172 (1997).....	10
<i>United States v. Aref</i> , 533 F.3d 72 (2d Cir. 2008)	6
<i>United States v. Libby</i> , 432 F. Supp. 2d 26, 31 (D.D.C. 2006)	17, 18
<i>United States v. Litvak</i> , 808 F.3d 160 (2d Cir. 2015)	10
<i>United States v. MacKey</i> , 647 F.2d 898 (9th Cir. 1981).....	17
<i>United States v. Millan</i> , 817 F. Supp. 1072 (S.D.N.Y. 1993).....	7
<i>United States v. Nixon</i> , 418 U.S. 683 (1974).....	<i>passim</i>
<i>United States v. Schulte</i> , 2022 WL 1639282 (S.D.N.Y. May 24, 2022)	7
<i>United States v. Siegel</i> , 1997 WL 12804 (S.D.N.Y. Jan. 14, 1997)	6
<i>United States v. Skelos</i> , 988 F.3d 645 (2d Cir. 2021)	12
<i>United States v. W.R. Grace</i> , 439 F. Supp. 2d 1125 (D. Mon. 2006).....	6
<i>United States v. Weigand</i> , 520 F. Supp. 3d 609 (S.D.N.Y. 2021)	5
<i>Van Loon v. Dep’t of Treasury</i> , 122 F.4th 549 (5th Cir. 2024)	15

STATUTES & RULES

Fed. R. Evid. 401	7, 14
Fed. R. Evid. 801	18
Fed. R. Evid. 803	18
Fed. R. Evid. 804	18, 19
Fed. R. Crim. P. 17	12
Fed. R. Crim. P. 45	12

OTHER AUTHORITIES

<https://git-scm.com/> (last accessed June 6, 2025)..... 12

The Peraire-Buenos’ subpoena seeks specific, relevant, potentially admissible documents from the only alleged victim who has been identified by anything other than a pseudonym. These documents are important for the Peraire-Buenos to meet the Superseding Indictment’s (“Indictment”) allegations and advance their defenses.

As discussed in greater detail below, Non-Party 1’s arguments miss the mark. Non-Party 1’s professed concerns about producing proprietary information are entirely resolved by the Protective Order in this case. Non-Party 1’s baseless suggestion (ECF 93 (Mot.) at 4, 7) that the Peraire-Buenos will use the requested computer code to hack Non-Party 1 reflects a deep misunderstanding of what allegedly happened in this case. The Peraire-Buenos are not alleged to have “hacked” anything; their alleged trading strategy depended on a *publicly available* alleged “vulnerability” in the MEV-Boost software, which was as visible to Non-Party 1 as it was to the Peraire-Buenos.

Non-Party 1’s arguments on the *Nixon* factors are similarly infirm. Non-Party 1 devotes much of its motion to disputing the relevance of requests that go to the core of the government’s case, including the very code that comprises the bot that was allegedly deceived and the sandwich strategy that the Peraire-Buenos allegedly thwarted. In other instances, Non-Party 1 objects to requests that seek communications with [REDACTED]

[REDACTED]. And although it accuses the Peraire-Buenos of a “fishing expedition,” Non-Party 1 neither argues that the documents do not exist (nor could it) nor credibly suggests that the requests are so broad as to call for an expansive set of responsive material.

For similar reasons, Non-Party 1’s claims of burden ring hollow. Non-Party 1 does not argue that it does not understand what documents the Peraire-Buenos seek or know where those

documents are located. Its claims of burden with respect to the computer-code requests are especially problematic. Assuming that identifying the version of Non-Party 1’s code in place at the time of the alleged “Exploit” will take some work, the supposed burden of that work is not “undue.” The code is so central to the government’s case—the Indictment makes multiple claims about how the code was deceived and the coded conditions it supposedly contained—that it is surprising that the *government* did not obtain the documents before pursuing an indictment. Non-Party 1 is the only source of these documents critical to the Peraire-Buenos’ defenses.

Taking a step back, Non-Party 1’s claim that it should not have to produce *any* of the documents sought by the subpoena is remarkable. Non-Party 1 is not a disinterested third party.

[REDACTED]

[REDACTED]. Now, [REDACTED]

[REDACTED] it seeks to deny the Peraire-Buenos the corresponding right to defend against the novel claims in the Indictment.

For these and all the reasons discussed in more detail below, the Court should deny Non-Party 1’s Motion to Quash.

BACKGROUND

As discussed in greater detail in the Peraire-Buenos’ Motions to Dismiss and other Motions filed concurrently therewith, *see* ECF 49, 51, 53, 55, and their Motion for Issuance of a Pretrial Return Subpoena (“Subpoena Motion”), *see* ECF 74, the Indictment charges the Peraire-Buenos with wire fraud and money laundering in connection with a novel trading strategy, which it calls the “Exploit,” on the Ethereum Network that allegedly disrupted the trading strategies of three

alleged Victim Traders. Non-Party 1 is the only one of the three alleged Victim Traders¹ who is known to the government or the defendants.

The Indictment alleges that the alleged Victim Traders used “automated” computer programs (bots) to direct and execute their trading strategy, Indict. ¶ 13; indeed, it is likely that all of the steps leading to the Victim Traders’ transactions (proposed and actual) were accomplished through pre-programmed computer code. The Indictment alleges that the transactions were submitted to builders with “coded conditions” that supposedly impacted the Victim Traders’ expectations regarding what could happen to the proposed bundles of transactions after they were submitted to builders. *Id.* ¶ 24. The Indictment further alleges that the alleged Victim Traders’ sandwich attack trading strategies were “typical[]” and characterizes them as “arbitrage.” *Id.* ¶¶ 13, 22. Because the Indictment does not allege any direct communication between the Peraire-Buenos and any Victim Trader, *see id.* ¶¶ 14-15, 24-27, its allegations (along with other government filings) indicate that the government will seek to prove that the Peraire-Buenos violated the purported norms or implicit expectations among the various users of the at-issue software on the Ethereum Network. As the government explained its theory in its Reply to its Motion for Reconsideration: “[T]he defendants made misrepresentations because the Victims were relying on the expectation that their trades would be executed only in a particular order.” ECF 91 at 12.

The Indictment also makes allegations about the Peraire-Buenos’ intent that go beyond the mechanics of the transactions. It alleges that the Peraire-Buenos took steps to conceal their identity

¹ It is not clear whether the Indictment alleges that the victims were the computer programs (the “MEV Bots”) or the individuals or companies associated with them. *Compare* Indict. ¶ 17 (defining the “Victim Traders” as “MEV Bots”), *with id.* ¶ 22 (defining the Victim Traders as “searchers who operate MEV Bots”).

and that this desire for anonymity is indicative of criminal intent. *E.g.*, Indict. ¶ 2. It also alleges that, after the alleged Exploit, the Peraire-Buenos refused to return the cryptocurrency they gained in the alleged trading strategy, despite being requested to do so by the alleged Victim Traders and a “representative from Ethereum.” *Id.* ¶ 30.

Non-Party 1 [REDACTED]. In the investigation that followed, it voluntarily provided some information and documents to the government, including:

- Select and redacted communications [REDACTED]
[REDACTED] (*see* Requests 4 and 5);
- Select communications [REDACTED]
[REDACTED]
[REDACTED] (*see* Request 6);
- Select communications [REDACTED]
[REDACTED] (*see* Request 7); and
- Select analysis [REDACTED]
[REDACTED] (*see* Request 7).

Before indicting the case, the government did not acquire, either through voluntary disclosure or grand jury subpoena, the source code that launched the sandwich attack (Request 1) or the source code of the smart contracts that Non-Party 1 used to execute their transactions (Request 2).

ARGUMENT

Non-Party 1 has no valid grounds to oppose the production, pursuant to the Protective Order, of a discrete set of documents and communications that lie at the heart of this case. Its arguments variously misconstrue the law, the subpoena’s requests, and the Indictment’s

allegations—and often all three. As an initial matter, there is no basis to quash the subpoena for any confidentiality concerns the Protective Order addresses. Moreover, the subpoena easily satisfies *Nixon*’s requirements of relevance, potential admissibility, and specificity. *See United States v. Nixon*, 418 U.S. 683, 700 (1974). Given the centrality of the requested evidence to the case and Non-Party 1’s voluntary production of certain documents to the government, the narrowly tailored subpoena does not pose an undue burden. The Court should deny the Motion to Quash in its entirety.

I. THE PROTECTIVE ORDER SUFFICIENTLY ADDRESSES CONCERNS ABOUT CONFIDENTIAL BUSINESS INFORMATION.

Without any legal authority, Non-Party 1 argues that it should not be required to produce documents in response to the subpoena because the information is proprietary. This objection is not a valid basis to quash or modify the subpoena.

First, the Protective Order in this case provides ample protection to any proprietary information that Non-Party 1 may produce in response to the subpoena. *See* ECF No. 25. The Peraire-Buenos will consent to the application of the Protective Order to productions made by Non-Party 1. The Protective Order includes multiple levels of protection—including levels for sealed material, attorneys’ possession only material, and attorneys’ eyes only material. It requires that protected material be filed under seal and precludes such material from being used in other circumstances and for purposes other than defending against the charges in this case. Confidentiality orders are commonly used in litigation to protect the confidential information of parties and non-parties alike, including in criminal cases. *See, e.g., United States v. Weigand*, 520 F. Supp. 3d 609, 615 (S.D.N.Y. 2021) (confidentiality objections did not justify quashing a subpoena because “a protective order is in place to preserve the confidentiality of such documents until trial,” and trial exhibits would be considered at the appropriate time).

Second, Non-Party 1's purported concerns (Mot. at 4, 7) that, notwithstanding the Protective Order, the Peraire-Buenos might misuse its proprietary information are entirely baseless. The Peraire-Buenos are not charged with a hacking crime, such as gaining unauthorized access to any computer systems or altering computer code. Rather, the alleged "vulnerability" in the MEV-Boost software that they allegedly used in connection with the "Exploit" was publicly available for anyone to identify and use for trading. Moreover, the Peraire-Buenos have complied with the Protective Order for over a year, with no problems. And pursuant to their conditions of release, the Peraire-Buenos are not permitted to trade cryptocurrency. The Peraire-Buenos do not seek this information for any untoward purpose, and Non-Party 1 has no basis to make that unsupported accusation.

Third, Non-Party 1's confidentiality concerns do not trump the Peraire-Buenos' constitutional rights. As discussed in the Peraire-Buenos' Subpoena Motion and below, the documents called for by the subpoena are highly relevant to the case. Courts considering arguments about the disclosure of confidential and proprietary information have found that a criminal defendant's need for the evidence overcomes a third party's interest in confidentiality, especially where a confidentiality order is in place. *See United States v. Siegel*, 1997 WL 12804, at *4 (S.D.N.Y. Jan. 14, 1997) (finding that the defendant's "need for the documents in preparing and presenting a complete defense" overcame third party's confidentiality concerns but incorporating safeguards such as the limitation of review to attorneys and experts).²

² The principle that a defendant's constitutional rights in a criminal case can overcome other privileges exists in other contexts as well. For example, courts have held that there are circumstances where attorney-client privilege must yield to a defendant's Sixth Amendment rights, *see, e.g., United States v. W.R. Grace*, 439 F. Supp. 2d 1125, 1136-41 (D. Mon. 2006); there are procedures for classified information to be disclosed to defense counsel in national securities cases, *e.g., United States v. Aref*, 533 F.3d 72, 78 (2d Cir. 2008); and deliberative process privilege must give way to a criminal defendant's rights, *see United States v. Nixon*, 418 U.S. 683, 712-13 (1974).

II. THE COURT SHOULD DENY THE MOTION TO QUASH AS TO THE REQUESTS FOR SOURCE CODE (REQUESTS 1-3).

As the Peraire-Buenos explained in their Subpoena Motion, Requests 1 through 3 seek the computer code that constructed the sandwich attacks that the Peraire-Buenos are alleged to have illegally thwarted.³ These requests easily clear the *Nixon* hurdles. *See* ECF 74 at 7-8. Focusing on Requests 1 and 2, Non-Party 1 challenges the Peraire-Buenos' showing as to relevancy, claims the requests are overbroad, and argues it would be subject to undue burden. None of these arguments has merit.

A. The Source Code for the MEV-Bot and the Smart Contracts Is Relevant.

Under *Nixon* and the Federal Rules of Evidence, relevance is a broad concept. Relevance is satisfied under Rule 17 if there is a “rational inference that at least part of the [materials] relate to the offenses charged in the indictment.” *Nixon*, 418 U.S. at 700. “Evidence is relevant [at trial] if it has *any tendency* to make a fact” of consequence more or less likely. Fed. R. Evid. 401 (emphasis added). Evidence may be relevant to a defense if it negates arguments advanced by the government. *See, e.g., United States v. Schulte*, 2022 WL 1639282, at *9 (S.D.N.Y. May 24, 2022) (“[A]lthough Defendant’s motive and intent are not elements of the offense with which he is charged, the Government may open the door to evidence of the sort that Defendant seeks to offer if it argues that Defendant was motivated by a desire to start an ‘information war’ with the United States.”); *United States v. Millan*, 817 F. Supp. 1072, 1082-83 (S.D.N.Y.) (ruling evidence admissible “if for no other reason than the fact that [the Government] made the evidence relevant

³ Specifically, these requests seek the MEV Bot code that directed the alleged proposed transactions (Request 1); the code that constituted the smart contracts for the alleged proposed transactions (Request 2); and the transmissions to and from the builder (Request 3). Non-Party 1 does not specifically challenge Request 3. Therefore, there is no basis to quash that request.

through . . . [its] opening statement and trial strategy” (citation omitted)), *modified sub nom. United States v. Millan-Colon*, 836 F. Supp. 1007 (S.D.N.Y. 1993).

As the Peraire-Buenos explained in their Subpoena Motion, *see* ECF 74 at 7-8, the source code for the MEV Bot and the smart contracts is plainly relevant. As noted above, the Indictment alleges that transactions in this trading environment primarily occur through smart contracts, which are computer code, Indict. ¶ 7, and that trades occur using automated bots (MEV Bots), which are also computer code, *id.* ¶ 13. With respect to the transactions at issue here, the Indictment alleges the proposed bundles had coded conditions reflecting a “typical[]” “bundle,” and it relies on those supposed conditions to allege that the alleged Victim Traders did not expect what happened during the alleged “Exploit.” *Id.* ¶¶ 13, 24, 26(c). These are not mere background allegations; the Indictment appears to rely on alleged expectations and norms (and alleged breach thereof) for its theories of falsity and materiality. *See id.* ¶¶ 24, 26(c); *accord* ECF 91 at 12 (“the Victims were relying on the expectation that their trades would be executed only in a particular order”); *id.* at 12-13 (“defendants’ actions were designed to and did take advantage of the expected rules and protocols of the particular software at issue”).

Non-Party 1 nevertheless argues that the documents “do not bear on material facts.” Mot. at 1. This argument appears to conflate relevance under *Nixon* with significance or materiality. That is incorrect, as *Nixon* only requires that the documents “relate” to the allegations. *Supra* p. 7. In any event, the code is material to the Peraire-Buenos’ defense under any sense of the word. Although the Peraire-Buenos need not disclose their trial strategy to meet the low relevance threshold, a few examples demonstrate the importance of this evidence.

First, having the source code will allow the Peraire-Buenos to challenge the government’s allegations that Non-Party 1’s MEV Bot and its smart contracts were programmed to operate in

the way the Indictment alleges.⁴ If the alleged Victim Traders are supposed to have been defrauded as a result of statements made by the Peraire-Buenos,⁵ and the alleged Victim Traders are supposed to have acted entirely through their MEV Bot to create proposed bundles via smart contracts, the requested materials would reveal the alleged Victim Traders' purported expectations for the trades at issue.

Second, the coded conditions (or lack of coded conditions) in the transactions are also relevant to the materiality of the alleged misrepresentations because they will identify the kinds of risks and conditions anticipated by the Victim Traders' strategy. As the Peraire-Buenos have indicated in other pleadings, as part of their defenses, they may highlight that one feature of the trading environment is its adversarial nature, and the kinds of risks the Victim Traders coded for is relevant to that argument, and it is also relevant to whether, for what purpose, and to what extent a participant would rely on the protocols referenced in the Indictment. Indict. ¶¶ 12-15. For all these reasons,⁶ these requests easily satisfy *Nixon*'s relevancy requirement.

Non-Party 1 argues that the Victim Traders' *subjective* expectations are not relevant because the standard for materiality is *objective*. But the government's case turns on a theory of thwarted expectations,⁷ and the subjective expectations of the alleged Victim Traders, as

⁴ Non-Party 1 makes the irrelevant claim that there is no "material dispute" about the "mechanics of the trade." Mot. at 5. There is no "material dispute" requirement in *Nixon*. See *supra* p.4-5. This argument also misunderstands the burden of proof in a criminal case. At trial, the government will have the burden to prove, and the Peraire-Buenos have the right to challenge, the Indictment's allegations about the mechanics of the trades and the conditions allegedly coded in the Victim Traders' desired trades.

⁵ The Indictment does not adequately allege any false statement sufficient to sustain a fraud charge. See ECF 49 at 21-25.

⁶ At trial, the Peraire-Buenos may advance additional relevance arguments for these documents.

⁷ To be clear, the Peraire-Buenos do not concede that evidence of "expectations" would be sufficient to prove wire fraud. But if the government is permitted to put on evidence regarding its

participants in the market, bear on the objective expectations of users in the relevant trading environment. *Cf., e.g., United States v. Litvak*, 808 F.3d 160, 175-76, 184 (2d Cir. 2015) (finding subjective testimony relevant to objective materiality determination in securities fraud context). This is especially true here, where Non-Party 1, whose MEV Bot is alleged to have engaged in “typical[]” trading, is the only sandwicher in the case that has been identified. Indict. ¶ 13. The fact that different evidence relevant to expectations may be available from other sources does not make the evidence the Peraire-Buenos seek here less relevant. *See Old Chief v. United States*, 519 U.S. 172, 179 (1997) (ruling that “evidentiary relevance under Rule 401” is not “affected by the availability of alternative proofs of the element to which it went,” though such consideration may bear on prejudice and cumulativeness). Because the government is relying on a theory of tacit expectations and alleged norms, and not on the alleged violations of written laws or regulations or on any other express directives to users of the Ethereum Network, there is no readily available “objective standard” to point to, and the defense is entitled to all relevant evidence available to rebut the government’s allegations—flawed as those allegations may be.

B. The Publicly Available Bytecode and Literature on the MEV-Boost System Do Not Provide the Requested Information.

Non-Party 1 notes (Mot. at 7) that the bytecode for the relevant smart contracts is publicly available. This statement is accurate but does not fully address what is sought by Request 2. Unlike the bytecode, the *source code* is not publicly available, and the source code provides key information here. Source code is the software written by developers in a programming language. It is compiled into the bytecode, the machine-readable representation of the source code, which is

allegations about what Non-Party 1 “expected” to happen, as the government’s filings have suggested it will seek to do, the Peraire-Buenos must have the opportunity to present a defense to those allegations.

then deployed to the block chain. The source code contains information, such as the way the smart contract is organized, function naming, and comments, that are lost when compiling into the bytecode. The “body of literature about protocols of relays and the functioning of MEV-Boost system,” Mot. at 8, obviously does not contain such information either.

C. Requests 1-3 Are Not Overbroad.

Non-Party 1 argues that the computer-code requests are overbroad, especially with respect to the MEV Bot code, and the Peraire-Buenos should only seek portions of the code. Because the Indictment does not allege *how* the MEV Bot determines or accomplishes its trading strategy (just that it does), the Peraire-Buenos are entitled to the entirety of the MEV Bot code. That said, the Peraire-Buenos acknowledge that there may be some portions of the MEV Bot code that could be excluded from production without causing them undue prejudice. If the Court is concerned about the breadth of this request, the Peraire-Buenos would be willing to limit this request to the portions of the code that govern how the MEV Bots (1) identify potential transactions in the mempool for a sandwich attack, (2) set the parameters for the transaction calls to their smart contracts, (3) construct and sign the transactions, (4) handle communications with the builder, (5) determine when or if a given trade should be cancelled, and (6) use consensus-level information (such as the “block signature”) in its trading decisions. An additional solution could be that Non-Party 1 provides a map of the modules for the MEV Bot’s code. The Peraire-Buenos could identify which modules are needed, so long as the process does not jeopardize the Peraire-Buenos’ ability to comply with expert deadlines. For example, load balancing modules are not needed.⁸

⁸ If producing more limited code is what Non-Party 1 prefers, it should not be heard to complain about the supposed burden of parsing its own code for this purpose.

D. Non-Party 1 Does Not Face Undue Burden.

Non-Party 1’s final objection to providing the source code is that it would be “difficult and burdensome.” Federal Rule of Criminal Procedure 17(c)(2) (unlike Federal Rule of Criminal Procedure 45(d)(1)) does not expressly reference a third party’s burden; rather, it asks whether a subpoena is “unreasonable or oppressive.” Courts assess whether a request is “unreasonable or oppressive” under Rule 17(c)(2) with reference to the *Nixon* standard, *see United States v. Skelos*, 988 F.3d 645, 661 (2d Cir. 2021), with burden arguments typically addressed under the “specificity” factor. As discussed, these requests clear the *Nixon* hurdles. Non-Party 1’s undue burden arguments also fail on their own merits.

First, as discussed above, the requests seek documents that are core to the Indictment’s allegations and are important for the Peraire-Buenos’ defenses. Second, the requests seek documents that can only be obtained from Non-Party 1. Third, the requests ask for the source code as of a specific date, not over a range of dates, which will ease the burden. It is standard practice in the development of code to use a version control system, which will save versions and identify changes via a changelog with dates on it. In referencing “commits” and “branches,” *see* Decl. ISO Non-Party 1’s Mot. ¶ 5, Non-Party 1 has acknowledged that it uses a version control system.⁹ The fact that Non-Party 1 will be required to do some work to respond to these requests does not make its burden “undue.” Non-Party 1 is not a disinterested third party; [REDACTED]

[REDACTED]. Fourth, the subpoena does not require Non-Party 1 to recreate market inputs or simulate precisely what the code did; the code itself is relevant for the reasons already stated.

⁹ An example of a version control system is Git. <https://git-scm.com/> (last accessed June 6, 2025).

Finally, the purported need for “scrubbing” does not make the burden undue. Given the Protective Order and other circumstances, *see* Section I, *supra*, such scrubbing is entirely unnecessary (and would be inappropriate if the information scrubbed is responsive to the requests).

E. If the Court Quashes Requests 1-3, the Government Should Be Precluded from Presenting Evidence or Argument on These Issues.

If Non-Party 1 is not required to produce documents responsive to Requests 1-3, the Court should preclude the government from presenting evidence or argument regarding the alleged conditions of the requested trades purportedly submitted by the Victim Traders to the builders, or the expectations that purportedly arose from, or are reflected by, those conditions. The government should not be permitted to argue that the Peraire-Buenos allegedly deceived the alleged Victim Traders if the defense is not able to review the code that was purportedly deceived. Likewise, the government should not be permitted to argue that the Victim Traders were denied certain trades due to the “Exploit” if the Peraire-Buenos cannot review the coded conditions that instructed the transaction to perform or not perform these trades. The Peraire-Buenos should not be subject to criminal prosecution based on such allegations if they are denied the ability to put on a complete defense. And the government should not benefit from its failure to gather—much less, to confirm—information core to its allegations through a grand jury subpoena.

III. THE COURT SHOULD DENY THE MOTION TO QUASH AS TO THE REQUESTS FOR COMMUNICATIONS (REQUESTS 4-7).

As the Peraire-Buenos established through the Subpoena Motion, the communications requests easily clear the *Nixon* standard.

A. The Communications Are Relevant.

Requests 4-7 seek limited communications pertaining to the alleged Exploit that Non-Party 1 had with various entities. (Request 4 seeks an unredacted copy of an already-produced set of communications that contains many redactions.) As the Peraire-Buenos explained in their

Subpoena Motion, at a minimum these communications are relevant to show [REDACTED] [REDACTED] and other participants in the trading environment, including the expectations of users of the Ethereum Network and MEV Boost.

Non-Party 1 makes several arguments challenging relevancy, including that (1) the Peraire-Buenos' Subpoena Motion did not list any examples of relevant communications, so there must not be any; (2) [REDACTED] are not "elements of the crime"; (3) the expectations of participants are not relevant to the case because the "social acceptability" of sandwiching is not at issue; and (4) "post-Exploit" communications are not relevant. These arguments misunderstand the legal standard, the Indictment's allegations, or both.

With respect to the legal standard, evidence does not have to negate an "element of the crime" to meet the *Nixon* standard or Federal Rule of Evidence 401, *see supra* p. 7, and the Peraire-Buenos are not required to disclose every possible use of a document for a subpoena to be valid. The requested communications are plainly relevant to the Indictment's allegations regarding the post-Exploit events, including the Peraire-Buenos' supposed "reject[ion]" of the Victim Traders' "requests to return the stolen cryptocurrency" and "steps" allegedly taken "to hide their ill-gotten gains," Indict. ¶ 1; *see id.* ¶¶ 28-32, because they show [REDACTED] [REDACTED] [REDACTED] [REDACTED].

Non-Party 1's other relevance arguments ignore key allegations in the Indictment.

- For example, the Indictment alleges that actions allegedly taken by the Peraire-Buenos to conceal their identity demonstrates intent to defraud. *E.g.*, Indict. ¶ 17. The Peraire-

Buenos are entitled to challenge those allegations, including by pointing out that pseudonymity is a widespread value and practice in the trading environment. *See, e.g., Van Loon v. Dep't of Treasury*, 122 F.4th 549, 554-55 (5th Cir. 2024) (pseudonymity); *id.* at 559 (identifying legitimate reasons for using mixers to provide additional anonymity).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].¹⁰

- As another example, the expectations of participants in the trading environment as to whether the alleged Exploit was legal, or even wrong, is relevant to the Peraire-Buenos' arguments about constitutional notice.¹¹ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].

- Non-Party 1's post-Exploit communications are relevant because the Indictment alleges that the post-Exploit actions of the Peraire-Buenos demonstrate intent to defraud

¹⁰ [REDACTED]

[REDACTED] The concern expressed in footnote 3 is unfounded.

¹¹ For the reasons explained in the Peraire-Buenos' Motions to Dismiss, these constitutional arguments are suitable for pre-trial resolution. But should the Court deny the Motion to Dismiss, the Peraire-Buenos still should be allowed to establish a record showing the lack of fair notice.

(retroactively) and/or to launder illicitly acquired funds—including the fact that they did not return the funds when asked to do so by the sandwichers or other participants in the Ethereum Network. Indict. ¶ 30. The government has also characterized actions taken by others in the Ethereum Network, such as Tether’s decision to freeze some of the crypto, as indicative of illegal behavior by the Peraire-Buenos. *See, e.g.*, ECF 91 at 8. The Peraire-Buenos are entitled to challenge those allegations, including by pointing out other reasons why such actions may or may not have been taken. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

B. Non-Party 1 Provides No Basis for the Redactions at Issue in Request 4.

Request 4 seeks the unredacted version of a document already produced—[REDACTED]

[REDACTED]. Other than an argument that the redacted information [REDACTED] is not relevant because it (like [REDACTED]) is “post-

Exploit,” Non-Party 1 identifies no basis for the redactions. Non-Party 1 should be required to produce the unredacted document.¹²

C. The Specificity Requirement Is Satisfied, and the Requests Are Tailored in Time and Subject Matter.

The requests for communications also satisfy *Nixon*’s specificity requirement: they seek communications that indisputably exist, and the requests are limited by time and subject matter. Non-Party 1 does not argue that communications with the identified entities do not exist. Non-Party 1 also does not claim that it provided to the government the full record of communications about the alleged Exploit with the identified entities. As a result, Non-Party 1 effectively concedes this *Nixon* requirement.

Nixon requires no more. The specificity requirement does not demand that criminal defendants identify with precision every relevant document they seek from a third party; rather, it is there to prevent true fishing expeditions for documents that are unknown to exist at all. *United States v. Libby*, 432 F. Supp. 2d 26, 31-32 (D.D.C. 2006) (noting that *Nixon* recognizes “it may be impossible to ‘describe fully’ the documents” and “therefore, the Court concluded that the specificity requirement could be satisfied if there is a ‘sufficient likelihood,’ demonstrated through rational inferences, that the documents being sought contain relevant and admissible evidence”); see *United States v. MacKey*, 647 F.2d 898, 901 (9th Cir. 1981) (noting that while a Rule 17(c) subpoena is not intended “to allow a blind fishing expedition seeking unknown evidence,” where the subpoenaing party demonstrated relevancy but had not yet seen the documents, “it would be

¹² Non-Party 1 does not oppose the subpoena on the ground that it seeks assertedly privileged documents. If Non-Party 1 nevertheless intends to assert privilege claims as to documents it is ordered to produce as it suggests it might, see Mot. at 14 n.4, it should be required to do so immediately and with specificity given [REDACTED]

unreasonable to expect a more detailed connection be provided between the contents of the documents and the ultimate facts at issue in the case”).

Non-Party 1’s characterization of these requests as expansive and untethered to the case disregards the actual requests. The requests are time limited and subject-matter limited. The Peraire-Buenos do not seek every communication [REDACTED], or every communication about sandwich trading. Non-Party 1 already selectively gathered and produced the communications *it* wanted the government to see. It is only fair that Non-Party 1—as interested of a non-party as one could be—be required to produce the remainder of the communications *with the same parties and on the same subject matter*.

D. The Communications Are Potentially Admissible.

Communications [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Non-Party 1’s admissibility arguments demand too much at this stage. Relying on cases where the defendant subpoenaed police investigatory material and civil cases addressing trial motions, *see* Mot. at 10-11, Non-Party 1 argues that the Peraire-Buenos will need to make a greater showing before using the documents at trial. At that stage, the admissibility of any evidence will depend on both the nature of the document itself and the specific purpose for which it is offered. But, at this stage, the inquiry is simply whether the documents are *arguably* admissible. *See Libby*, 432 F. Supp. 2d at 31; *Nixon*, 418 U.S. at 700 (requiring a “sufficient preliminary showing”). To be clear, however, the requested material has more than speculative evidentiary use. In addition

to the uses already discussed above and in the Subpoena Motion, the communications likely will be admissible as statements against interest under Federal Rule of Evidence 804(b)(3). [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

IV. THE COURT SHOULD DENY THE MOTION TO QUASH AS TO REQUESTS 8 AND 9.

Requests 8 and 9 seek specific documents relevant to the Indictment’s allegations that the alleged victims were engaged in “typical[]” trading and its allegations about the makeup and expectations of individuals trading on the Ethereum Network.

Non-Party 1 mainly argues that the identification of other sandwich bots owned by Non-Party 1 and the financial reports that identify the amount of money made by those bots are not relevant. For some of the same reasons discussed above and for some new reasons, Non-Party 1’s arguments are unavailing.

First, as noted above, the *Indictment alleges* that the alleged Victim Traders are engaged in “typical[]” “arbitrage” and sets up sandwich trades as typical MEV trading. These allegations are used in the Indictment—and will presumably be used at trial—to portray the alleged “Exploit” as a broad threat to the stability of the Ethereum Network and to tie the alleged practices of the Victim Traders to the industry norms. The Peraire-Buenos are entitled to challenge the story told by the Indictment as to what is a typical trader, what is a typical trade, and what typical traders

¹³ See [REDACTED].

expect—especially because, as noted above, the purported violation of those alleged expectations and norms is a central part of the government’s argument as to why the alleged Exploit constituted wire fraud. If the government is wrong as to what is typical, or what is arbitrage, or what traders expect, that error undermines the government’s ability to prove its case.¹⁴

Second, as the Peraire-Buenos have previously explained, *see* ECF 51 at 10-13, the Peraire-Buenos do not, as Non-Party 1 suggests, seek this information “to distract the jury from their own crimes,” Mot. at 15. The exploitative nature of sandwich trading bears on the norms and expectations in the trading environment (which the evidence will show is adversarial and trustless) and the potential information the alleged “Lure Transactions” could have conveyed (or lack thereof). They are also relevant to the Peraire-Buenos’ constitutional notice arguments.

Third, the identification of other Non-Party-1-controlled sandwich bots is relevant because it will allow the Peraire-Buenos to place those trades in the context of the broader trading volume that can be assessed using publicly available information. As noted in the Peraire-Buenos’ Subpoena Motion (at 11), research has shown that over 75% of sandwich trades are associated with just 20 accounts. It would be relevant to what is “typical” and what the objective expectations are, for example, if Non-Party 1 controlled a substantial proportion of the sandwich bots active on the Ethereum Network or a large volume of the sandwich exploits on a decentralized network with many more trades. This is not mere speculation: the Peraire-Buenos may show that many traders have decided not to operate sandwich strategies because of moral or legal reservations, and,

¹⁴ Non-Party 1’s arguments mischaracterize the relevant Indictment allegations. Paragraph 13 of the Indictment alleges that *searchers* engage in arbitrage by proposing bundles, which are “typically” sandwich trades. Contrary to Non-Party 1’s characterization, Paragraph 13 does *not* say that this is a typical means by which *some* searchers pursue arbitrage. Mot. at 15 n.5.

[REDACTED]

[REDACTED]. Because only Non-Party 1 has been identified among the alleged Victim Traders, it is the only source of this kind of information.

CONCLUSION

The subpoena seeks relevant, specific, potentially admissible evidence that is important to the Peraire-Buenos' ability to defend themselves. Non-Party 1, as the only identified alleged victim, is an important and interested third party. After voluntarily and selectively providing some information to the government, Non-Party 1 should not be heard to complain about the supposedly undue burden of producing the additional relevant information that it has withheld. Its concerns about confidentiality are adequately resolved by the Protective Order. The Court should deny the Motion to Quash.

Date: June 6, 2025

Respectfully submitted,

By: /s/ Katherine Trefz

By: /s/ Daniel N. Marx

Katherine Trefz (*pro hac vice*)
Daniel Shanahan (*pro hac vice*)
Patrick J. Looby (*pro hac vice*)
Williams & Connolly LLP
680 Maine Avenue SW
Washington, DC 20024
Tel: (202) 434-5000
ktrefz@wc.com
dshanahan@wc.com
plooby@wc.com

Daniel N. Marx
William W. Fick (*pro hac vice*)
Fick & Marx LLP
24 Federal Street, 4th Floor
Boston, MA 02110
Tel: 857-321-8360
dmarx@fickmarx.com
wfick@fickmarx.com

*Counsel for Defendant
Anton Peraire-Bueno*

Jonathan P. Bach
Shapiro Arato Bach
1140 Avenue of the Americas
17th Floor
New York, NY 10036
Tel: 212-257-4897
jbach@shapiroarato.com

*Counsel for Defendant
James Peraire-Bueno*

CERTIFICATE OF SERVICE

I hereby certify that on June 6, 2025, I electronically filed the foregoing document with the Clerk of Court using the CM/ECF system which will send notification of such filing to all counsel of record in this matter who are on the CM/ECF system.

/s/ Katherine Trefz
Katherine Trefz